

PENDETEKSIAN SERANGAN
MAC ADDRESS DENGAN MENGGUNAKAN WIDS
(WIRELESS INTRUSION DETECTION SYSTEM)
BERBASIS SNORT
SKRIPSI



Oleh :

HANDUNG FIRSTO TAMA
1034010041

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNOLOGI INDUSTRI
UNIVERSITAS PEMBANGUNAN NASIONAL
"VETERAN" JAWA TIMUR
2014

SKRIPSI
PENDETEKSIAN SERANGAN
MAC ADDRESS DENGAN MENGGUNAKAN WIDS
(WIRELESS INTRUSION DETECTION SYSTEM)
BERBASIS SNORT

Disusun Oleh :

HANDUNG FIRSTO TAMA

1034010041

Telah dipertahankan dihadapan dan diterima oleh Tim Penguji Skripsi
Program Studi Teknik Informatika Fakultas Teknologi Industri
Universitas Pembangunan Nasional "Veteran" Jawa Timur
Pada Tanggal : 21 Februari 2014

Pembimbing :

Tim Penguji :

1.

1.

Made Suartana, S.Kom, M.Kom.

Dr. Ir. Ni Ketut Sari, MT.

NIP. 19650731 199203 2 001

2.

2.

Henni Endah Wahanani, ST., M.Kom.

Budi Nugroho, S.Kom, M.Kom.

NPT. 3 7809 130 348 1

NPT. 3 8006 050 205 1

3.

Achmad Junaidi, S.Kom.

NPT. 3 7811 040 199 1

Mengetahui
Dekan Fakultas Teknologi Industri
Universitas Pembangunan Nasional "Veteran" Jawa Timur
Surabaya


Ir. Sutiyono, MT

NIP. 19600713 198703 1 001

Judul : PENDETEKSIAN SERANGAN MAC ADDRESS
DENGAN MENGGUNAKAN WIDS (WIRELESS
INTRUSION DETECTION SYSTEM) BERBASIS SNORT

Pembimbing I : I Made Suartana, S.Kom, M.Kom.

Pembimbing II : Henni Endah W, ST, M.Kom.

Penyusun : Handung Firsto Tama

ABSTRAK

Keamanan jaringan nirkabel atau wireless yang semakin pesat membuatnya rentan dalam sejumlah ancaman keamanan terutama dengan menggunakan metode WIDS (Wireless Intrusion Detection System). Salah satu ancaman keamanan dalam WIDS (Wireless Intrusion Detection System) adalah spoofing ancaman tersebut merubah MAC address.

Pada umumnya MAC address tidak dapat diubah karena sudah ditetapkan oleh NIC (Network Interface Card) dan sudah dimasukkan ke dalam ROM (hardware). Akan tetapi ada beberapa kartu jaringan menyediakan utilitas yang memungkinkan pengguna untuk merubah MAC address, meski hal tersebut kurang disarankan. Perubahan MAC address akan dilakukan untuk memecahkan masalah di atas.

Solusinya peneliti dapat melakukan perubahan MAC address dalam satu ROM (hardware) dan dapat terdeteksi oleh detector. Detector snort disiapkan untuk melakukan analisa serangan MAC address spoofing. Hasilnya dalam analisa, detector snort masih mampu mendeteksi serangan MAC address spoofing dan dengan analisa koefisien cohen's kappa yang digunakan untuk menghitung reliabilitas antar dua rater. Hasil yang didapat adalah $k=0.516$ dengan katagori cukup (fair).

Kata Kunci : MAC address spoofing, WIDS, snort

KATA PENGANTAR

Puji syukur penulis panjatkan kehadirat Allah SWT yang telah memberikan segala nikmat dan karunia-Nya sehingga penulis dapat menyelesaikan skripsi tepat pada waktunya. Serta atas limpahan rahmat yang tak terhingga penulisan laporan skripsi yang berjudul “Pendeteksian Serangan MAC Address Dengan Menggunakan WIDS (Wireless Intrusion Detection System) Berbasis Snort” dapat terselesaikan.

Skripsi ini dibuat sebagai salah satu syarat memperoleh gelar sarjana komputer di jurusan teknik informatika UPN “Veteran” Jatim. Selesaiannya skripsi ini juga berkat dukungan semua pihak. Oleh karena itu, penulis ingin mengucapkan terima kasih kepada:

1. Ayah dan Bunda selaku orang tua yang paling tercinta, terima kasih atas semua doa, dukungan, serta banyak hal lain yang tidak bisa di ucapkan satu per satu, tanpa dukungan dari kalian penulis tidak yakin bisa menyelesaikan skripsi ini tepat waktu. Terima kasih sebanyak-banyaknya atas semuanya. Dan penulis memohon doa agar setelah lulus dari perguruan tinggi dan menyandang gelar sarjana komputer, penulis mampu menjadi lebih bermanfaat bagi orang lain dan dapat membahagiakan keluarga terutama orang tua.
2. Bapak Prof. Dr. Ir. Teguh Soedarto, MP., selaku Rektor Universitas Pembangunan Nasional “Veteran” Jawa Timur.

3. Bapak Ir. Muttasim Billah, MS., selaku Wakil Dekan Fakultas Teknologi Industri Universitas Pembangunan Nasional “Veteran” Jawa Timur.
4. Ibu Dr. Ir. Ni Ketut Sari, MT., selaku Ketua Jurusan Teknik Informatika Universitas Pembangunan Nasional “Veteran” Jawa Timur.
5. Bapak I Made Suartana, S.Kom, M.Kom., selaku dosen pembimbing satu. Terima kasih karena telah banyak memberikan arahan, bimbingan, serta meluangkan waktu dalam membimbing penulis untuk mengerjakan skripsi ini.
6. Ibu Henni Endah W, ST., M.Kom., selaku dosen pembimbing dua. Terima kasih karena telah banyak memberikan arahan, bimbingan, serta meluangkan waktu dalam membimbing penulis untuk mengerjakan skripsi ini.
7. Pacarku Holifatus Sofi, terima kasih banyak telah memberikan motivasi dan dukungan dari awal pengajuan skripsi hingga skripsi ini selesai, serta menjadi penghibur hati saat sedang kacau mengerjakan skripsi.
8. Teman-teman seangkatan 2010 Angga, Indra, Genta, Mifta, Bapak Pringga, Davi, Po po, Hamid, dan banyak lagi teman-teman yang tidak bisa di sebutkan satu-persatu. Terima kasih semuanya kerana sudah memotivasi penulis sampai menyelesaikan skripsi ini.

Penulis menyadari skripsi ini masih jauh dari kata sempurna, sehingga saran dan kritik yang membangun sangat berguna bagi penulis. Semoga laporan skripsi ini bermanfaat bagi pembaca dan semua orang yang membutuhkan referensi.

Akhirnya, penulis berharap agar penyusun laporan ini mampu memberikan sumbangsih bagi perkembangan dan kemajuan Teknik Informatika Universitas Pembangunan Nasional “Veteran” Jawa Timur.

Surabaya, 21 Februari 2014

Penulis

DAFTAR ISI

ABSTRAK	i
KATA PENGANTAR	ii
DAFTAR ISI	v
DAFTAR GAMBAR	viii
DAFTAR TABEL	xii
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Perumusan Masalah	2
1.3 Batasan Masalah	3
1.4 Tujuan dan Manfaat	3
1.5 Sistematika Laporan	4
BAB II TINJAUAN PUSTAKA	6
2.1 Penelitian Terdahulu	6
2.2 Landasan Teori	7
2.2.1 Jaringan Komputer	7
2.2.2 Internet	7
2.2.3 Wireless	9
2.2.4 Keamanan Wireless	10
2.2.5 Serangan Wireless	10
2.2.6 Tentang Rule	12
2.2.7 Model OSI Layer	12

2.2.8	Wireless Network	15
2.2.9	Intrusion Detection System (IDS)	15
2.2.10	Wireless Intrusion Detection System (WIDS)	16
2.2.11	Snort	17
2.2.12	ARP Spoofing	17
2.2.13	Virtualbox	18
2.2.14	Cain And Abel	18
2.2.15	Technitium MAC Address Changer	18
2.2.16	Router	19
2.2.17	Koefisien Cohen'n Kappa	19
BAB III	METODELOGI PENELITIAN	21
3.1	Rancangan Penelitian	21
3.1.1	Studi Literatur	22
3.1.2	Definisi Kebutuhan Sistem	22
3.1.3	Rancangan Implementasi	24
3.2	Rancangan Uji Coba Dan Evaluasi	28
3.2.1	Skenario 1 (satu)	29
3.2.2	Skenario 2 (dua)	30
3.3	Rancangan Analisa Pembuktian Serangan	34
BAB IV	HASIL DAN PEMBAHASAN	36
4.1	Implementasi	36
4.1.1	Install Sistem Operasi	37
4.1.2	Connect Wireless LAN	38
4.1.3	Ping IP Address	38

4.1.4	Install Library Libpcap	40
4.1.5	Install Library Libdnet	42
4.1.6	Install Library Daq	44
4.1.7	Ekstrak dan Install Snort	45
4.1.8	Konfigurasi Snort	47
4.1.9	Install dan Konfigurasi Barnyard2	53
4.1.10	Setup MYSQL	55
4.1.11	Konfigurasi BASE (Basic Analysis and Security Engine)	57
4.2	Hasil Uji Coba dan Evaluasi	59
4.2.1	Hasil Uji Coba Skenario Satu	59
4.2.2	Hasil Uji Coba Skenario Dua	63
4.2.3	Analisa Serangan	72
BAB V	KESIMPULAN DAN SARAN	83
5.1	Kesimpulan	83
5.2	Saran	83

DAFTAR PUSTAKA

LAMPIRAN

DAFTAR GAMBAR

Gambar 2.1	Struktur Tujuh Lapisan Model OSI	13
Gambar 3.1	Alur Rancangan Penelitian	21
Gambar 3.2	Rancangan Topologi Jaringan	25
Gambar 3.3	Alur Rancangan Topologi	26
Gambar 3.4	Alur Rancangan Implementasi Snort	27
Gambar 3.5	Skenario 1 (satu)	29
Gambar 3.6	Skenario 2 (dua) Perubahan MAC Address	31
Gambar 3.7	Skenario 2 (dua) Serangan Dengan MAC Yang Berbeda.	32
Gambar 3.8	Alur Rancangan Analisa Pembuktian Serangan	34
Gambar 4.1	Instalasi Sistem	36
Gambar 4.2	Install Sistem Operasi	37
Gambar 4.3	Connect Wireless LAN	38
Gambar 4.4	Test Ping Ubuntu 11.10	39
Gambar 4.5	Test Ping Windows 7	40
Gambar 4.6	Proses Ekstrak Library Libpcap	41
Gambar 4.7	Proses Install Library Libpcap	41
Gambar 4.8	Proses Ekstrak Library Libdnet	42
Gambar 4.9	Proses Install Library Libdnet	43
Gambar 4.10	Proses Ekstrak Library Daq	44
Gambar 4.11	Proses Install Library Daq	45
Gambar 4.12	Proses Ekstrak Snort	46
Gambar 4.13	Proses Install Snort	46

Gambar 4.14	Konfigurasi Masuk Ke Direktori snort.conf	48
Gambar 4.15	Line HOME_NET	48
Gambar 4.16	Line EXTERNAL_NET	49
Gambar 4.17	Line RULE_PATH	50
Gambar 4.18	Line WHITE_LIST	50
Gambar 4.19	Line BLACK_LIST	51
Gambar 4.20	Line Output Unified2	52
Gambar 4.21	Line RULE_PATH	52
Gambar 4.22	Proses Install Barnyard2	54
Gambar 4.23	Proses Konfigurasi Barnyard2	55
Gambar 4.24	Create Database	56
Gamabr 4.25	Show Tables	56
Gambar 4.26	Step 1 Konfigurasi BASE	58
Gambar 4.27	Tampilan BASE (Basic Analysis and Security Engine) ..	58
Gambar 4.28	Korban Belum Terjadi Serangan Arpspoof	60
Gambar 4.29	Tool Cain And Abel Attack Arpspoof	61
Gambar 4.30	Serangan Arpspoof	61
Gamabr 4.31	Duplikat MAC address	62
Gambar 4.32	Detector Snort Mendeteksi Serangan Arpspoof	62
Gambar 4.33	Running Snort Dan Barnyard2	65
Gambar 4.34	Change MAC Address	65
Gambar 4.35	Serangan MAC Address Spoofing	66
Gambar 4.36	Displaying Alert	67
Gambar 4.37	Korban Belum Terjadi Serangan Arpspoof	68

Gambar 4.38	Tool Cain And Abel Attack Arpspoof	69
Gambar 4.39	Serangan Arpspoof	69
Gambar 4.40	Duplikat MAC Address	70
Gambar 4.41	Detector Snort Mendeteksi Serangan Arpspoof	70
Gambar 4.42	Menunjukkan Waktu Dan Alert	72
Gambar 4.43	Displaying Alert	73
Gambar 4.44	Log Percobaan Pertama Dari Analisa Serangan MAC Address	75
Gambar 4.45	Log Percobaan Kedua Dari Analisa Serangan MAC Address	75
Gambar 4.46	Log Percobaan Ketiga Dari Analisa Serangan MAC Address	75
Gambar 4.47	Log Percobaan Keempat Dari Analisa Serangan MAC Address	75
Gambar 4.48	Log Percobaan Kelima Dari Analisa Serangan MAC Address	75
Gambar 4.49	Log Percobaan Keenam Dari Analisa Serangan MAC Address	75
Gambar 4.50	Log Percobaan Ketujuh Dari Analisa Serangan MAC Address	76
Gambar 4.51	Log Percobaan Kedelapan Dari Analisa Serangan MAC Address	76
Gambar 4.52	Log Percobaan Kesembilan Dari Analisa Serangan MAC Address	76

Gambar 4.53	Log Percobaan Kesepuluh Dari Analisa Serangan MAC	
	Address	76
Gambar 4.54	Jumlah MAC Address Yang Terdeteksi	77
Gambar 4.55	SPSS Analisa Kappa	88

DAFTAR TABEL

Tabel 2.1	7 Lapisan Model OSI	14
Tabel 2.2	Transformasi Kappa	19
Tabel 3.1	List IP	25
Tabel 4.1	Analisa Serangan	73
Tabel 4.2	Tiga Puluh Kali Analisa Serangan Dengan Kesempatan Pertama	77
Tabel 4.3	Tiga Puluh Kali Analisa Serangan Dengan Kesempatan Kedua	82
Tabel 4.4	Analisa Kappa	86

BAB I

PENDAHULUAN

1.1 LATAR BELAKANG

Seiring dengan penyebaran jaringan nirkabel (wireless network) berkaitan dengan komunikasi antar sistem komputer tanpa menggunakan kabel. Jaringan nirkabel ini sering dipakai untuk jaringan komputer baik pada jarak yang dekat (beberapa meter, memakai alat atau pemancar bluetooth) maupun pada jarak jauh (lewat satelit). Bidang ini erat hubungannya dengan bidang telekomunikasi, teknologi informasi, dan teknik komputer. Jenis jaringan yang populer dalam katagori jaringan nirkabel adalah jaringan kawasan lokal nirkabel (wireless LAN/WAN), dan Wi-Fi. Jaringan nirkabel biasanya menghubungkan satu sistem komputer dengan sistem yang lain dengan menggunakan beberapa macam media transmisi tanpa kabel, seperti gelombang radio, gelombang mikro, maupun cahaya infra merah.

Keamanan jaringan nirkabel atau wireless yang semakin pesat membuatnya rentan terhadap sejumlah ancaman keamanan. Jaringan wireless bisa jadi merupakan hal terakhir yang tidak terpikirkan. Pada umumnya bertujuan untuk mendapatkan koneksi internet pada saat connect ke jaringan wireless, akan tetapi banyak juga yang melakukan untuk maksud-maksud tertentu mulai dari keingintahuan, coba-coba, dan research. Salah satu ancaman keamanan dalam wireless adalah spoofing ancaman tersebut merubah IP address dan MAC address. IP addresss (Internet Protocol) merupakan protokol dasar untuk mengirim data melalui jaringan internet dan banyak jaringan komputer lainnya.

MAC address merupakan kode keras pada Network Interface Controller (NIC) dan tidak dapat di ubah. Namun ada alat (software) yang dapat membuat sistem operasi percaya bahwa NIC memiliki MAC address yang dapat memilih sendiri oleh pengguna.

Dari penelitian jurnal, peneliti mencoba melakukan serangan dengan cara memalsukan layanan jaringan nirkabel klien. Dengan menggunakan metode Wireless Intrusion Detection System (WIDS). WIDS merupakan sebuah perangkat lunak ataupun perangkat keras yang digunakan untuk akses yang tidak sah dari sebuah sistem komputer atau jaringan. Dalam penerapannya, metode WIDS (Wireless Intrusion Detection System) menggunakan tools snort-wireless yang berjalan pada sistem operasi linux. Sistem tersebut diuji dengan serangan Man In The Middle Attack berupa ARP spoofing. Paket serangan dapat dilihat melalui monitoring paket berbasis web. (Tasmil, 2012)

Dalam penelitian jurnal sebelumnya pengamanan menggunakan WIDS (Wireless Intrusion Detection System) belum cukup untuk mengamankan serangan, khususnya terhadap serangan ARP spoofing yang menyusup melalui MAC address. Oleh karena itu di dalam sekripsi ini, serangan MAC address akan diperbanyak untuk memaksimalkan pendeteksian serangan. Serangan MAC address nantinya akan dilakukan sebanyak enam puluh kali untuk pengujian serangan agar WIDS (Wireless Intrusion Detection System) menjadi lebih aman dan mampu mendeteksi serangan dari attacker.

1.2 PERUMUSAN MASALAH

Dari latar belakang diatas maka dirumuskan permasalahan dalam tugas akhir ini adalah sebagai berikut:

1. Bagaimana mengimplementasikan detector snort dengan menggunakan virtual?
2. Bagaimana cara mendeteksi serangan MAC address dengan menggunakan tool snort di WIDS (Wireless Intrusion Detection System)?
3. Bagaimana mendokumentasi serangan yang telah dilakukan attacker?

1.3 BATASAN MASALAH

Batasan masalah yang ada di penelitian ini adalah:

1. Detector hanya menggunakan virtual.
2. Serangan menggunakan ARP spoofing yang di fokuskan ke pendeteksian MAC address spoofing.
3. Penyerangan hanya menggunakan satu device.
4. Pendeteksian serangan hanya menggunakan tool snort.
5. Jaringan wireless yang digunakan hanya menggunakan jaringan lokal class C.

1.4 TUJUAN DAN MANFAAT

Adanya tujuan dan manfaat dalam penyusunan skripsi ini sebagai berikut:

1.4.1 Tujuan

1. Dapat mengimplementasikan detector snort dengan menggunakan virtual.
2. Dapat mendeteksi serangan MAC address dengan menggunakan tool snort di WIDS (Wireless Intrusion Detection System).
3. Dapat mendokumentasikan serangan yang dilakukan oleh attacker.

1.4.2 Manfaat

Manfaat yang diperoleh dalam mendeteksi Wireless Intrusion Detection System antara lain :

- a. Bagi penulis bermanfaat untuk menerapkan pengetahuan yang di peroleh selama menempuh bangku perkuliahan.
- b. Bagi mahasiswa bermanfaat untuk mengenal lebih jauh tentang ilmu pendeteksian di wireless.
- c. Bagi pembaca bermanfaat menambah informasi tentang pendeteksian wireless dan sebagai bahan literatur lebih lanjut.

1.5 SISTEMATIKA LAPORAN

Laporan skripsi ini terbagi dari 5 (lima) bab, dimana masing-masing bab terdiri dari beberapa sub-bab yang menjelaskan isi dari bab-bab tersebut. Adapun sistematika penulisan laporan ini sebagai berikut:

1. BAB I PENDAHULUAN

Pada bab pendahuluan ini menguraikan hal-hal yang berkaitan dengan masalah-masalah yang dihadapi oleh penulis, antara lain: latar belakang permasalahan, perumusan masalah, batasan masalah dan tujuan skripsi.

2. BAB II TINJAUAN PUSTAKA

Pada bab ini menjelaskan hal-hak yang berkaitan dengan teori antara lain: penelitian terdahulu, landasan teori.

3. BAB III METODE PENELITIAN

Pada bab ini menjelaskan metode-metode yang dilakukan saat penelitian skripsi berlangsung yang meliputi: rancangan penelitian, rancangan uji coba

dan evaluasi, dan jadwal penelitian (bentuk chart). Rancangan penelitian akan di bagi lagi menjadi: studi literatur, definisi kebutuhan sistem, dan rancangan implementasi.

4. BAB IV HASIL DAN PEMBAHASAN

Pada bab ini berisi tentang pembahasan sebuah Pendeteksian Serangan MAC address dengan menggunakan WIDS (Wireless Intrusion Detection System) berbasis snort. Mulai dari cara kerja hingga bagian-bagian yang terdapat pada sistem tersebut meliputi: implementasi, hasil uji coba dan evaluasi.

5. BAB V KESIMPULAN

Bab ini berisi kesimpulan dan saran yang sekiranya dapat bermanfaat bagi pembaca.